Authors:
N. Benamar   J. Härri   J. Lee   T. Ernst
Moulay Ismail University of Meknes   *EURECOM*   *Sangmyung University*   *YoGoKo*

RFC 8691
Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11

Abstract

This document provides methods and settings for using IPv6 to communicate among nodes within range of one another over a single IEEE 802.11-OCB link. Support for these methods and settings require minimal changes to existing stacks. This document also describes limitations associated with using these methods. Optimizations and usage of IPv6 over more complex scenarios are not covered in this specification and are a subject for future work.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8691.

Copyright Notice

with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document provides a baseline for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link [IEEE-802.11-2016] (a.k.a., 802.11p; see Appendices A, B, and C) with minimal changes to existing stacks. Moreover, the document identifies the limitations of such usage. Concretely, the document describes the layering of IPv6 networking on top of the IEEE Std 802.11 MAC layer or an IEEE Std 802.3 MAC layer with a frame translation underneath. The resulting stack is derived from IPv6 over Ethernet [RFC2464] but operates over 802.11-OCB to provide at least P2P (point-to-point) connectivity using IPv6 Neighbor Discovery (ND) and link-local addresses.

The IPv6 network layer operates on 802.11-OCB in the same manner as operating on the Ethernet with the following exceptions:

- Exceptions due to the different operation of the IPv6 network layer on 802.11 compared to the Ethernet. The operation of IP on Ethernet is described in [RFC1042] and [RFC2464].
- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure, and movement detection. Security and privacy recommendations are discussed in Sections 4.4 and 5. The subnet structure is described in Section 4.6. The movement detection on OCB links is not described in this document. Likewise, ND extensions and IP Wireless Access in Vehicular Environments (IPWAVE) optimizations for vehicular communications are not in scope of this document. The expectation is that further specifications will be edited to cover more complex vehicular networking scenarios.

The reader may refer to [IPWAVE] for an overview of problems related to running IPv6 over 802.11-OCB. It is out of scope of this document to reiterate those problems.

2. Terminology

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The document makes uses of the following terms:

IP-OBU (Internet Protocol On-Board Unit):
> An IP-OBU denotes a computer situated in a vehicle such as a car, bicycle, or similar. It has at least one IP interface that runs in mode OCB of 802.11 and has an "OBU" transceiver. See the definition of the term "OBU" in Appendix H.

IP-RSU (IP Roadside Unit):
> An IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU over an 802.11 wireless link operating in OCB mode. An IP-RSU is similar to an Access Network Router (ANR), defined in [RFC3753], and a Wireless Termination Point (WTP), defined in [RFC5415].

OCB (outside the context of a Basic Service Set - BSS):
> This is a mode of operation in which a station (STA) is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality.

802.11-OCB:
> This refers to the mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivited is 'true'.

3. Communication Scenarios Where IEEE 802.11-OCB Links Are Used

IEEE 802.11-OCB networks are used for vehicular communications as 'Wireless Access in Vehicular Environments'. In particular, we refer the reader to [IPWAVE], which lists some scenarios and requirements for IP in Intelligent Transportation Systems (ITS).

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. All links are assumed to be P2P, and multiple links can be on one radio interface. While 802.11-OCB is clearly specified and a legacy IPv6 stack can operate on such links, the use of the operating environment (vehicular networks) brings in new perspectives.

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11-OCB is inherited from [RFC2464] and, as such, is 1500 octets. As noted in [RFC8200], every link on the Internet must have a minimum MTU of 1280 octets and must follow the other recommendations, especially with regard to fragmentation.

4.2. Frame Format

IP packets **MUST** be transmitted over 802.11-OCB media as QoS data frames whose format is specified in an IEEE 802.11 spec [IEEE-802.11-2016].

The IPv6 packet transmitted on 802.11-OCB is immediately preceded by a Logical Link Control (LLC) header and an 802.11 header. In the LLC header and in accordance with EtherType Protocol Discrimination (EPD; see Appendix D), the value of the Type field **MUST** be set to 0x86DD (IPv6). The mapping to the 802.11 data service **SHOULD** use a 'priority' value of 1 (QoS with a 'Background' user priority), reserving higher priority values for safety-critical and time-sensitive traffic, including the ones listed in [ETSI-sec-archi].

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers **MAY** implement IPv6 over Ethernet as per [RFC2464] and then a frame translation from 802.3 to 802.11 in order to minimize the code changes.

4.3. Link-Local Addresses

There are several types of IPv6 addresses [RFC4291] [RFC4193] that may be assigned to an 802.11-OCB interface. Among these types of addresses, only the IPv6 link-local addresses can be formed using an EUI-64 identifier, particularly during transition time (the period of time before an interface starts using an address different from the LL one).

If the IPv6 link-local address is formed using an EUI-64 identifier, then the mechanism for forming that address is the same mechanism as that used to form an IPv6 link-local address on Ethernet links. Moreover, regardless of whether the interface identifier is derived from the EUI-64 identifier, its length is 64 bits, as is the case for the Ethernet [RFC2464].

4.4. Stateless Autoconfiguration

The steps a host takes in deciding how to autoconfigure its interfaces in IPv6 are described in [RFC4862]. This section describes the formation of Interface Identifiers for 'Global' or 'Unique Local' IPv6 addresses. Interface Identifiers for 'link-local' IPv6 addresses are discussed in Section 4.3.

The **RECOMMENDED** method for forming stable Interface Identifiers (IIDs) is described in [RFC8064]. The method of forming IIDs described in Section 4 of [RFC2464] **MAY** be used during transition time, particularly for IPv6 link-local addresses. Regardless of the method used to form the IID, its length is 64 bits, similarly to IPv6 over Ethernet [RFC2464].

The bits in the IID have no specific meaning, and the identifier should be treated as an opaque value. The bits 'Universal' and 'Group' in the identifier of an 802.11-OCB interface, which is an IEEE link-layer address, are significant. The details of this significance are described in [RFC7136].

Semantically opaque IIDs, instead of meaningful IIDs derived from a valid and meaningful MAC address ([RFC2464], Section 4), help avoid certain privacy risks (see the risks mentioned in Section 5.1.1). If semantically opaque IIDs are needed, they may be generated using the method for generating semantically opaque IIDs with IPv6 Stateless Address Autoconfiguration given in [RFC7217]. Typically, an opaque IID is formed starting from identifiers different from the MAC addresses and from cryptographically strong material. Thus, privacy-sensitive information is absent from Interface IDs because it is impossible to calculate back the initial value from which the Interface ID was first generated.

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose IIDs don't change too often. It is **RECOMMENDED** to use the mechanisms described in [RFC7217] to permit the use of stable IIDs that do not change within one subnet prefix. A possible source for the Net_Iface parameter is a virtual interface name or logical interface name that is decided by a local administrator.

4.5. Address Mapping

Unicast and multicast address mapping **MUST** follow the procedures specified for Ethernet interfaces described in Sections 6 and 7 of [RFC2464].

4.5.1. Address Mapping -- Unicast

This document is scoped for Address Resolution (AR) and Duplicate Address Detection (DAD) per [RFC4862].

4.5.2. Address Mapping -- Multicast

The multicast address mapping is performed according to the method specified in Section 7 of [RFC2464]. The meaning of the value "33-33" mentioned there is defined in Section 2.3.1 of [RFC7042].

Transmitting IPv6 packets to multicast destinations over 802.11 links proved to have some performance issues [IEEE802-MCAST]. These issues may be exacerbated in OCB mode. Future improvement to this specification should consider solutions for these problems.

4.6. Subnet Structure

When vehicles are in close range, a subnet may be formed over 802.11-OCB interfaces (not by their in-vehicle interfaces). A Prefix List conceptual data structure ([RFC4861], Section 5.1) is maintained for each 802.11-OCB interface.

The IPv6 Neighbor Discovery protocol (ND) requires reflexive properties (bidirectional connectivity), which is generally, though not always, the case for P2P OCB links. IPv6 ND also requires transitive properties for DAD and AR, so an IPv6 subnet can be mapped on an OCB

network only if all nodes in the network share a single physical broadcast domain. The extension to IPv6 ND operating on a subnet that covers multiple OCB links and does not fully overlap (i.e., non-broadcast multi-access (NBMA)) is not in scope of this document. Finally, IPv6 ND requires permanent connectivity of all nodes in the subnet to defend their addresses -- in other words, very stable network conditions.

The structure of this subnet is ephemeral in that it is strongly influenced by the mobility of vehicles: the hidden terminal effects appear, and the 802.11 networks in OCB mode may be considered ad hoc networks with an addressing model, as described in [RFC5889]. On the other hand, the structure of the internal subnets in each vehicle is relatively stable.

As recommended in [RFC5889], when the timing requirements are very strict (e.g., fast-drive-through IP-RSU coverage), no on-link subnet prefix should be configured on an 802.11-OCB interface. In such cases, the exclusive use of IPv6 link-local addresses is **RECOMMENDED**.

Additionally, even if the timing requirements are not very strict (e.g., the moving subnet formed by two following vehicles is stable, a fixed IP-RSU is absent), the subnet is disconnected from the Internet (i.e., a default route is absent), and the addressing peers are equally qualified (that is, it is impossible to determine whether some vehicle owns and distributes addresses to others), the use of link-local addresses is **RECOMMENDED**.

The baseline ND protocol [RFC4861] **MUST** be supported over 802.11-OCB links. Transmitting ND packets may prove to have some performance issues, as mentioned in Section 4.5.2 and Appendix I. These issues may be exacerbated in OCB mode. Solutions for these problems should consider the OCB mode of operation. Future solutions to OCB should consider solutions for avoiding broadcast. The best of current knowledge indicates the kinds of issues that may arise with ND in OCB mode; they are described in Appendix I.

Protocols like Mobile IPv6 [RFC6275] [RFC3963] and DNAv6 [RFC6059], which depend on timely movement detection, might need additional tuning work to handle the lack of link-layer notifications during handover. This topic is left for further study.

5. Security Considerations

Any security mechanism at the IP layer or above that may be implemented for the general case of IPv6 may also be implemented for IPv6 operating over 802.11-OCB.

The OCB operation does not use existing 802.11 link-layer security mechanisms. There is no encryption applied below the network layer running on 802.11-OCB. At the application layer, the IEEE 1609.2 document [IEEE-1609.2] provides security services for certain applications to use; application-layer mechanisms are out of scope of this document. On the other hand, a security mechanism provided at the networking layer, such as IPsec [RFC4301], may provide data security protection to a wider range of applications.

802.11-OCB does not provide any cryptographic protection because it operates outside the context of a BSS (no Association Request/Response or Challenge messages). Therefore, an attacker can sniff or inject traffic while within range of a vehicle or IP-RSU (by setting an interface card's

frequency to the proper range). Also, an attacker may not adhere to the legal limits for radio power and can use a very sensitive directional antenna; if attackers wish to attack a given exchange, they do not necessarily need to be in close physical proximity. Hence, such a link is less protected than commonly used links (a wired link or the aforementioned 802.11 links with link-layer security).

Therefore, any node can join a subnet and directly communicate with any nodes on the subset, including potentially impersonating another node. This design allows for a number of threats outlined in Section 3 of [RFC6959]. While not widely deployed, SEND [RFC3971] [RFC3972] is a solution that can address spoof-based attack vectors.

5.1. Privacy Considerations

As with all Ethernet and 802.11 interface identifiers [RFC7721], the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing, and IP hijacking risks. A vehicle embarking an IP-OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data. This may reveal data considered private by the vehicle owner; there is a risk of being tracked. In outdoor public environments, where vehicles typically circulate, the privacy risks are greater than in indoor settings. It is highly likely that attacker sniffers are deployed along routes that listen for IEEE frames, including IP packets, of vehicles passing by. For this reason, in 802.11-OCB deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses (Section 5.2), semantically opaque Interface Identifiers, and stable Interface Identifiers (Section 4.4). An example of a change policy is to change the MAC address of the OCB interface each time the system boots up. This may help mitigate privacy risks to a certain level. Furthermore, for privacy concerns, [RFC8065] recommends using an address-generation scheme rather than generating addresses from a fixed link-layer address. However, there are some specificities related to vehicles. Since roaming is an important characteristic of moving vehicles, the use of the same Link-Local Address over time can indicate the presence of the same vehicle in different places and thus lead to location tracking. Hence, a vehicle should get hints about a change of environment (e.g., engine running, GPS, etc.) and renew the IID in its LLAs.

5.1.1. Privacy Risks of Meaningful Information in Interface IDs

The privacy risks of using MAC addresses displayed in Interface Identifiers are important. IPv6 packets can be captured easily on the Internet and on-link on public roads. For this reason, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store, and correlate company ID information present in the MAC addresses of a large number of cars (e.g., listening for Router Advertisements or other IPv6 application data packets, and recording the value of the source address in these packets). Further correlation of this information with other data captured by other means or other visual information (e.g., car color) may constitute privacy risks.

5.2. MAC Address and Interface ID Generation

In 802.11-OCB networks, the MAC addresses may change during well-defined renumbering events. At the moment the MAC address is changed on an 802.11-OCB interface, all the Interface Identifiers of IPv6 addresses assigned to that interface **MUST** change.

Implementations should use a policy dictating when the MAC address is changed on the 802.11-OCB interface. For more information on the motivation of this policy, please refer to the privacy discussion in Appendix B.

A 'randomized' MAC address has the following characteristics:

- The "Local/Global" bit is set to "locally administered".
- The "Unicast/Multicast" bit is set to "Unicast".
- The 46 remaining bits are set to a random value using a random number generator that meets the requirements of [RFC4086].

To meet the randomization requirements for the 46 remaining bits, a hash function may be used. For example, the hash function defined in [SHA256] may be used with the input of a 256-bit local secret, the 'nominal' MAC address of the interface, and a representation of the date and time of the renumbering event.

A randomized Interface ID has the same characteristics of a randomized MAC address except for the length in bits.

5.3. Pseudonymization Impact on Confidentiality and Trust

Vehicle and drivers privacy relies on pseudonymization mechanisms such as the ones described in Section 5.2. This pseudonymization means that upper-layer protocols and applications **SHOULD NOT** rely on layer-2 or layer-3 addresses to assume that the other participant can be trusted.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[IEEE-802.11-2016]   IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems Local and metropolitan area networks-- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11-2016, December 2016, <https://standards.ieee.org/findstds/standard/802.11-2016.html>.

[RFC1042]

Postel, J. and J. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", STD 43, RFC 1042, DOI 10.17487/RFC1042, February 1988, <https://www.rfc-editor.org/info/rfc1042>.

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2464]   Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <https://www.rfc-editor.org/info/rfc2464>.

[RFC4086]   Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4191]   Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[RFC4193]   Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4291]   Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4301]   Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4861]   Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862]   Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC5415]   Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC6059]   Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", RFC 6059, DOI 10.17487/RFC6059, November 2010, <https://www.rfc-editor.org/info/rfc6059>.

[RFC6275]   Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[RFC7042]

Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042, October 2013, <https://www.rfc-editor.org/info/rfc7042>.

[RFC7136]   Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <https://www.rfc-editor.org/info/rfc7136>.

[RFC7217]   Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC8064]   Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8174]   Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200]   Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

7.2. Informative References

[CFR-90]   e-CFR, "Electronic Code of Federal Regulations", Title 47, Part 90 - PRIVATE LAND MOBILE RADIO SERVICES, <https://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.90&rgn=div5>.

[CFR-90.7]   e-CFR, "Electronic Code of Federal Regulations", Title 47, CFR 90.7 - Definitions, <https://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.90&rgn=div5#se47.5.90_17>.

[CFR-95]   e-CFR, "Electronic Code of Federal Regulations", Title 47, CFR 95 - PERSONAL RADIO SERVICES, <https://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.95&rgn=div5>.

[ETSI-sec-archi]   "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management", ETSI TS 102 940 V1.2.1, November 2016, <http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf>.

[IEEE-1609.2]   IEEE, "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages", DOI 10.1109/IEEESTD.2016.7426684, IEEE Standard 1609.2-2016, March 2016, <http://ieeexplore.ieee.org/document/7426684>.

[IEEE-1609.3]   IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services", DOI 10.1109/IEEESTD.2016.7458115, IEEE Standard 1609.3-2016, April 2016, <http://ieeexplore.ieee.org/document/7458115>.

[IEEE-1609.4]   IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation", DOI 10.1109/IEEESTD.2016.7435228, IEEE Standard 1609.4-2016, March 2016, <http://ieeexplore.ieee.org/document/7435228>.

[IEEE-802.11-2007]   IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", DOI 10.1109/IEEESTD.2007.373646, IEEE Standard 802.11-2007, June 2007, <https://ieeexplore.ieee.org/document/4248378>.

[IEEE-802.11-2012]   IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", DOI 10.1109/IEEESTD.2012.6178212, IEEE Standard 802.11-2012, March 2012, <https://ieeexplore.ieee.org/document/6419735>.

[IEEE-802.11p-2010]   IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments", DOI 10.1109/IEEESTD.2010.5514475, IEEE Standard 802.11p-2010, July 2010, <https://standards.ieee.org/standard/802_11p-2010.html>.

[IEEE-802.3-2012]   IEEE, "IEEE Standard for Ethernet", DOI 10.1109/IEEESTD.2012.6419735, IEEE Standard 802.3-2012, December 2012, <https://ieeexplore.ieee.org/document/6419735>.

[IEEE802-MCAST]   Perkins, C., McBride, M., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", Work in Progress, Internet-Draft, draft-ietf-mboned-ieee802-mcast-problems-11, 11 December 2019, <https://tools.ietf.org/html/draft-ietf-mboned-ieee802-mcast-problems-11>.

[IPWAVE]   Jeong, J., "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", Work in Progress, Internet-Draft, draft-ietf-ipwave-vehicular-networking-12, 3 October 2019, <https://tools.ietf.org/html/draft-ietf-ipwave-vehicular-networking-12>.

[RFC3753]   Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <https://www.rfc-editor.org/info/rfc3753>.

[RFC3963]   Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <https://www.rfc-editor.org/info/rfc3963>.

[RFC3971]

Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC3972]   Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[RFC5889]   Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <https://www.rfc-editor.org/info/rfc5889>.

[RFC6959]   McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <https://www.rfc-editor.org/info/rfc6959>.

[RFC7721]   Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <https://www.rfc-editor.org/info/rfc7721>.

[RFC8065]   Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <https://www.rfc-editor.org/info/rfc8065>.

[RFC8505]   Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

[SHA256]   National Institute of Standards and Technology, "Secure Hash Standard (SHS)", DOI 10.6028/NIST.FIPS.180-4, FIPS 180-4, August 2015, <https://csrc.nist.gov/publications/detail/fips/180/4/final>.

Appendix A.   802.11p

The term "802.11p" is an earlier definition. The behavior of "802.11p" networks is rolled in [IEEE-802.11-2016]. In that document, the term "802.11p" disappears. Instead, each 802.11p feature is conditioned by the IEEE Management Information Base (MIB) attribute "OCBActivated" [IEEE-802.11-2016]. Whenever OCBActivated is set to "true", the IEEE Std 802.11-OCB state is activated. For example, an 802.11 STAtion operating outside the context of a BSS has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix B.   Aspects Introduced by OCB Mode to 802.11

In IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. In OCB mode, the manner in which channels are selected and used is simplified compared to when in BSS mode. Contrary to BSS mode, at the link layer, it is necessary to statically set the same channel number (or

frequency) on two stations that need to communicate with each other (in BSS mode, this channel set operation is performed automatically during 'scanning'). The manner in which stations set their channel number in OCB mode is not specified in this document. Stations STA1 and STA2 can exchange IP packets only if they are set to the same channel. At the IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol. The allocation of a particular channel for a particular use is defined statically in standards authored by ETSI in Europe, the FCC in the United States of America, and similar organizations in South Korea, Japan, and other parts of the world.

Briefly, the IEEE 802.11-OCB mode has the following properties:

- The use by each node of a 'wildcard' BSS identifier (BSSID) (i.e., each bit of the BSSID is set to 1).
- No IEEE 802.11 beacon frames are transmitted.
- No authentication is required in order to be able to communicate.
- No association is needed in order to be able to communicate.
- No encryption is provided in order to be able to communicate.
- Flag dot11OCBActivated is set to "true".

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the radio communication range. The MAC CDMA function resolves any eventual conflict(s).

The message exchange diagram in Figure 1 illustrates a comparison between traditional 802.11 and 802.11 in OCB mode. The 'Data' messages can be IP packets such as HTTP or others. Other 802.11 management and control frames (non-IP) may be transmitted, as specified in the 802.11 standard. The names of these messages as currently specified by the 802.11 standard are listed in Appendix F.

```
   STA                      AP         STA1                     STA2
   |                        |           |                        |
   |<------ Beacon -------|           |<------ Data -------->|
   |                        |           |                        |
   |---- Probe Req. ---->|           |<------ Data -------->|
   |<--- Probe Res. ------|           |                        |
   |                        |           |<------ Data -------->|
   |---- Auth Req. ------>|           |                        |
   |<--- Auth Res. -------|           |<------ Data -------->|
   |                        |           |                        |
   |---- Asso Req. ------>|           |<------ Data -------->|
   |<--- Asso Res. -------|           |                        |
   |                        |           |<------ Data -------->|
   |<------ Data -------->|           |                        |
   |<------ Data -------->|           |<------ Data -------->|

      (i) 802.11 Infrastructure mode       (ii) 802.11-OCB mode
```
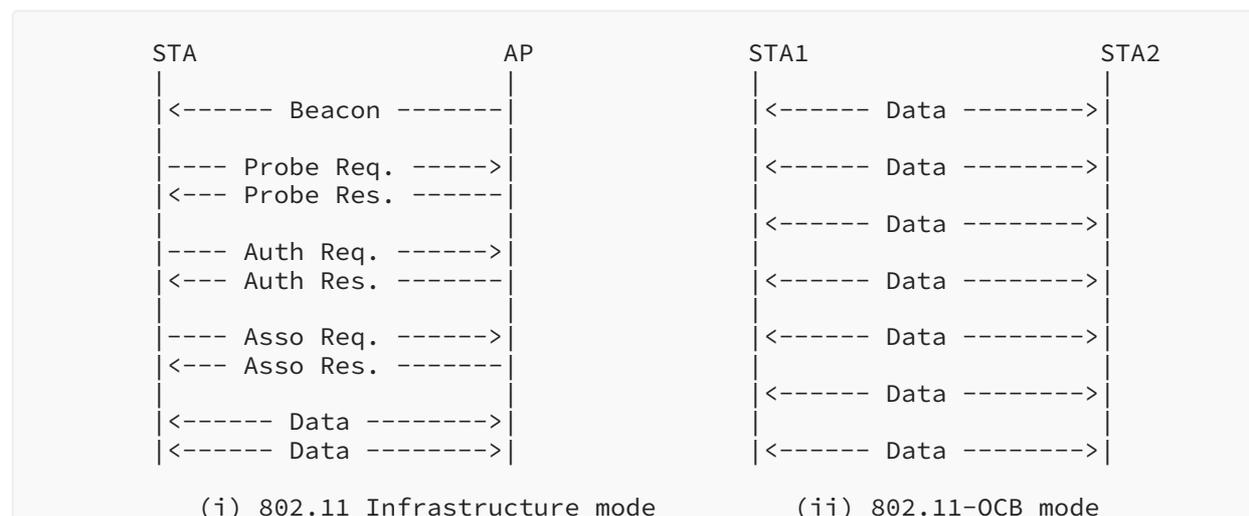
Figure 1: Difference between Messages Exchanged on 802.11 (Left) and 802.11-OCB (Right)

The 802.11-OCB interface was specified in [IEEE-802.11p-2010], Amendment 6: Wireless Access in Vehicular Environments, as an amendment to [IEEE-802.11-2007]. Since then, this amendment has been integrated into [IEEE-802.11-2012] and [IEEE-802.11-2016].

In [IEEE-802.11p-2010], anything qualified specifically as "OCBActivated" or "outside the context of a basic service" that is set to be "true" actually refers to OCB aspects introduced to 802.11.

In order to delineate the aspects introduced by 802.11-OCB to 802.11, we refer to the earlier [IEEE-802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n) but needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles and between vehicles and fixed infrastructure deployed along roads. While 'p' is a letter identifying the Amendment, just like 'a', 'b', 'g', and 'n' are, 'p' is concerned more with MAC modifications and is slightly concerned with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with Orthogonal Frequency Division Multiplexing (OFDM) at 5.4 GHz and 5.9 GHz.

The 802.11-OCB links are specified to be as compatible as possible with the behavior of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11-OCB MAC layer offers practically the same interface to IP as 802.11a/b/g/n and 802.3. A packet sent by an IP-OBU may be received by one or multiple IP-RSUs. The link-layer resolution is performed by using the IPv6 Neighbor Discovery protocol.

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11-OCB in the same way that IPv6 is layered on top of LLC on top of 802.11a/b/g/n (for WLAN) or on top of LLC on top of 802.3 (for Ethernet)), it is useful to analyze the differences between the 802.11-OCB and 802.11 specifications. During this analysis, we note that whereas 802.11-OCB lists relatively complex and numerous changes to the MAC layer (and very few to the PHY layer), there are only a few characteristics that may be important for an implementation transmitting IPv6 packets on 802.11-OCB links.

The most important 802.11-OCB aspect that influences the IPv6 functioning is the OCB characteristic; an additional, less direct influence is the maximum bandwidth afforded by the PHY modulation/demodulation methods and channel access specified by 802.11-OCB. The maximum bandwidth theoretically possible in 802.11-OCB is 54 Mbit/s (when using, for example, the following parameters: a 20 MHz channel; modulation of 64-QAM; a coding rate R of 3/4). With regard to IP over 802.11-OCB, in practice, a commonly observed figure is 12 Mbit/s; this bandwidth allows the operation of a wide range of protocols relying on IPv6.

- Operation outside the context of a BSS (OCB): The 802.11-OCB links (previously 802.11p) are operated without a BSS. This means that IEEE 802.11 beacon, Association Request/Response, Authentication Request/Response, and similar frames are not used. The used identifier of BSS (BSSID) always has a hexadecimal value of 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff; otherwise, the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by an administrator (e.g., 'My-Home-AccessPoint'). The OCB operation -- namely, the lack of beacon-based scanning and lack of authentication -- should be taken into account

when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

- Timing Advertisement: This is a new message defined in 802.11-OCB that does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time delivered by a Global Navigation Satellite System (GNSS) (e.g., Galileo, GPS, etc.) or by a cellular system. This message is optional for implementation.

- Frequency range: This is a characteristic of the PHY layer; it has almost no impact on the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ECC/CEPT based on ENs from ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11-OCB, the regulator associates a set of frequency ranges or slots within a band to the use of applications of vehicular communications in a band known as "5.9 GHz". The 5.9 GHz band is different from the 2.4 GHz and 5 GHz bands used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11-OCB in 5.9 GHz bands does not require a license in the EU (in the US, the 5.9 GHz is a licensed band of spectrum; for the fixed infrastructure, explicit FCC authorization is required; for an on-board device, a 'licensed-by-rule' concept applies, where rule certification conformity is required). Technical conditions are different from those of the "2.4 GHz" or "5 GHz" bands. The allowed power levels and, implicitly, the maximum allowed distance between vehicles is 33 dBm for 802.11-OCB (in Europe) compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1 km compared to approximately 50 m. Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in the US) and on the use of frequencies for Intelligent Transportation Systems (in the EU) compared to Wireless LAN (802.11a/b/g/n).

- 'Half-rate' encoding: As the frequency range, this parameter is related to PHY and thus does not have much impact on the interface between the IP layer and the MAC layer.

- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings, there is a strong need for a dynamic change of these addresses (as opposed to the non-vehicular settings -- real wall protection -- where fixed MAC addresses do not currently pose privacy risks). This is further described in Section 5. A relevant function is described in [IEEE-1609.3] and [IEEE-1609.4].

Appendix C. Changes Needed on an 802.11a Software Driver to Become an 802.11-OCB Driver

The 802.11p amendment modifies both the 802.11 stack's physical and MAC layers, but all the induced modifications can be quite easily obtained by modifying an existing 802.11a ad hoc stack.

The conditions for 802.11a hardware to be compliant with 802.11-OCB are as follows:

- The PHY entity shall be an OFDM system. It must support the frequency bands on which the regulator recommends the use of ITS communications -- for example, using an IEEE 802.11-OCB layer of 5875 MHz to 5925 MHz in France.

- The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- The chip transmit spectrum mask must be compliant with the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments do not require compliance).
- The chip should be able to transmit up to 44.8 dBm when used in the United States and up to 33 dBm in Europe; other regional conditions apply.

Changes needed on the network stack in OCB mode are as follows:

- Physical layer:

  ◦ Orthogonal frequency-division multiple access The chip must use the Orthogonal Frequency Division Multiple Access (OFDMA) encoding mode.
  ◦ The chip must be set to half-mode rate mode (the internal clock frequency is divided by two).
  ◦ The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules if used by the kernel to enforce local specific restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

- MAC layer:

  ◦ All management frames (beacons, join, leave, and others) emission and reception must be disabled, except for frames of subtype Action and Timing Advertisement (defined below).
  ◦ No encryption key or method must be used.
  ◦ Packet emission and reception must be performed as in ad hoc mode using the wildcard BSSID (ff:ff:ff:ff:ff:ff).
  ◦ The functions related to joining a BSS (Association Request/Response) and authentication (Authentication Request/Reply, Challenge) are not called.
  ◦ The beacon interval is always set to 0 (zero).
  ◦ Timing Advertisement frames, defined in the amendment, should be supported. The upper layer should be able to trigger such frames emission and retrieve information contained in the received Timing Advertisements.

Appendix D. Protocol Layering

A more theoretical and detailed view of layer stacking and interfaces between the IP layer and 802.11-OCB layers is illustrated in Figure 2. The IP layer operates on top of EtherType Protocol Discrimination (EPD). This discrimination layer is described in [IEEE-802.3-2012]. The interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

```
            +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
            |                IPv6                |
            +-+-+-+-+-{          }+-+-+-+-+-+-+-+
                      {  LLC_SAP  }               802.11-OCB
            +-+-+-+-+-{          }+-+-+-+-+-+-+-+  Boundary
            |          EPD          |     |     |
            |                     | MLME  |     |
            +-+-+-{  MAC_SAP   }+-+-+-|  MLME_SAP  |
            |       MAC Sublayer     |     |     |
            |      and ch. coord.    |     | SME | 802.11-OCB
            +-+-+-{   PHY_SAP   }+-+-+-+-+-+-|     | Services
            |                     | PLME  |     |
            |          PHY Layer    |  PLME_SAP  |
            +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
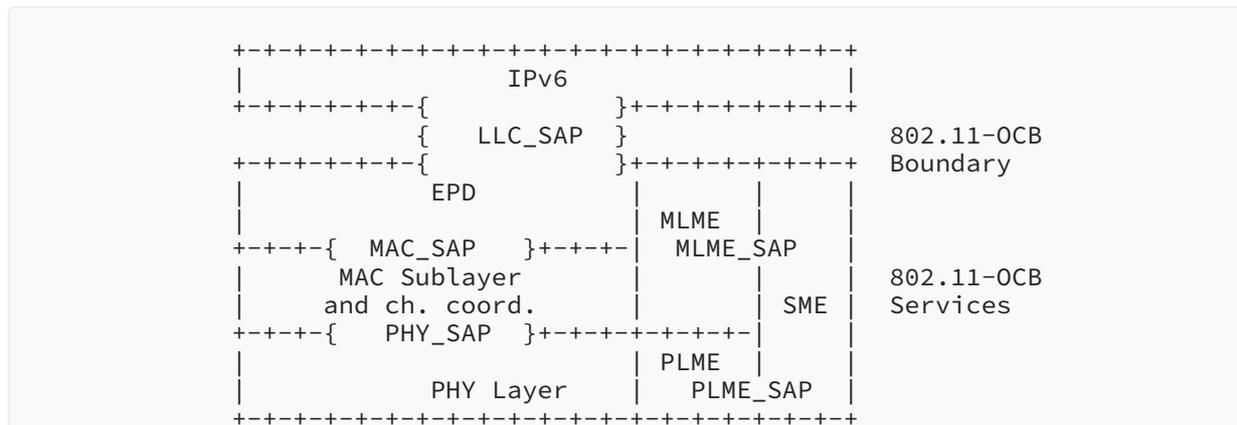
Figure 2: EtherType Protocol Discrimination

Appendix E.   Design Considerations

The networks defined by 802.11-OCB are in many ways similar to other networks of the 802.11 family. In theory, the transportation of IPv6 over 802.11-OCB could be very similar to the operation of IPv6 over other networks of the 802.11 family. However, the high mobility, strong link asymmetry, and very short connection makes the 802.11-OCB link significantly different from other 802.11 networks. Also, automotive applications have specific requirements for reliability, security, and privacy, which further add to the particularity of the 802.11-OCB link.

Appendix F.   IEEE 802.11 Messages Transmitted in OCB Mode

At the time of writing, this is the list of IEEE 802.11 messages that may be transmitted in OCB mode, i.e., when dot11OCBActivated is true in a STA:

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement.
- The STA may send control frames except those of subtype PS-Poll, CF-End, and CF-End plus CFAck.
- The STA **MUST** send data frames of subtype QoS Data.

Appendix G.   Examples of Packet Formats

This section describes an example of an IPv6 packet captured over an IEEE 802.11-OCB link.

By way of example, we show that there is no modification in the headers when transmitted over 802.11-OCB networks -- they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment for capturing an IPv6 packet on an 802.11-OCB link. In the topology depicted in Figure 3, the packet is an IPv6 Router Advertisement. This packet is emitted by a router on its 802.11-OCB interface. The packet is captured on the host using a network protocol analyzer (e.g., Wireshark). The capture is performed in two different modes: direct mode and monitor mode. The topology used during the capture is depicted below.

The packet is captured on the host. The host is an IP-OBU containing an 802.11 interface in Peripheral Component Interconnect (PCI) Express format (an Industrial Technology Research Institute (ITRI) product). The kernel runs the ath5k software driver with modifications for OCB mode. The capture tool is Wireshark. The file format for saving and analyzing is .pcap. The packet is generated by the router, which is an IP-RSU (an ITRI product).

```
            +--------+                             +-------+
            |        |      802.11-OCB Link         |       |
        ---|  Router |-----------------------------|  Host |
            |        |                             |       |
            +--------+                             +-------+
```

Figure 3: Topology for Capturing IP Packets on 802.11-OCB

During several capture operations running from a few moments to several hours, no messages relevant to the BSSID contexts were captured (Association Request/Response, Authentication Req/ Resp, or beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

Overall, the captured message is identical to a capture of an IPv6 packet emitted on an 802.11b interface. The contents are exactly the same.

G.1. Capture in Monitor Mode

The IPv6 RA packet captured in monitor mode is illustrated below. The Radiotap header provides more flexibility for reporting the characteristics of frames. The Radiotap header is prepended by this particular stack and operating system on the host machine to the RA packet received from the network (the Radiotap header is not present on the air). The implementation-dependent Radiotap header is useful for piggybacking PHY information from the chip's registers as data in a packet that is understandable by userland applications using socket interfaces (the PHY interface can be, for example, power levels, data rate, or the ratio of signal to noise).

The packet present on the air is formed by the IEEE 802.11 Data header, Logical Link Control header, IPv6 Base header, and ICMPv6 header.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Header Revision|  Header Pad   |       Header Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Present Flags                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data Rate     |              Pad                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: Radiotap Header v0

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type/Subtype and Frame Ctrl |          Duration              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Receiver Address...                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... Receiver Address          |      Transmitter Address...      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... Transmitter Address                                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          BSS ID...                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... BSS ID                   | Frag Number and Seq Number   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: IEEE 802.11 Data Header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     DSAP    |I|    SSAP     |C| Control Field | Org. Code...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... Organizational Code      |           Type               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6: Logical Link Control Header

```
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |Version| Traffic Class |              Flow Label               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Payload Length        |   Next Header  |   Hop Limit   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                                                               +
    |                                                               |
    +                       Source Address                          +
    |                                                               |
    +                                                               +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                                                               +
    |                                                               |
    +                    Destination Address                        +
    |                                                               |
    +                                                               +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
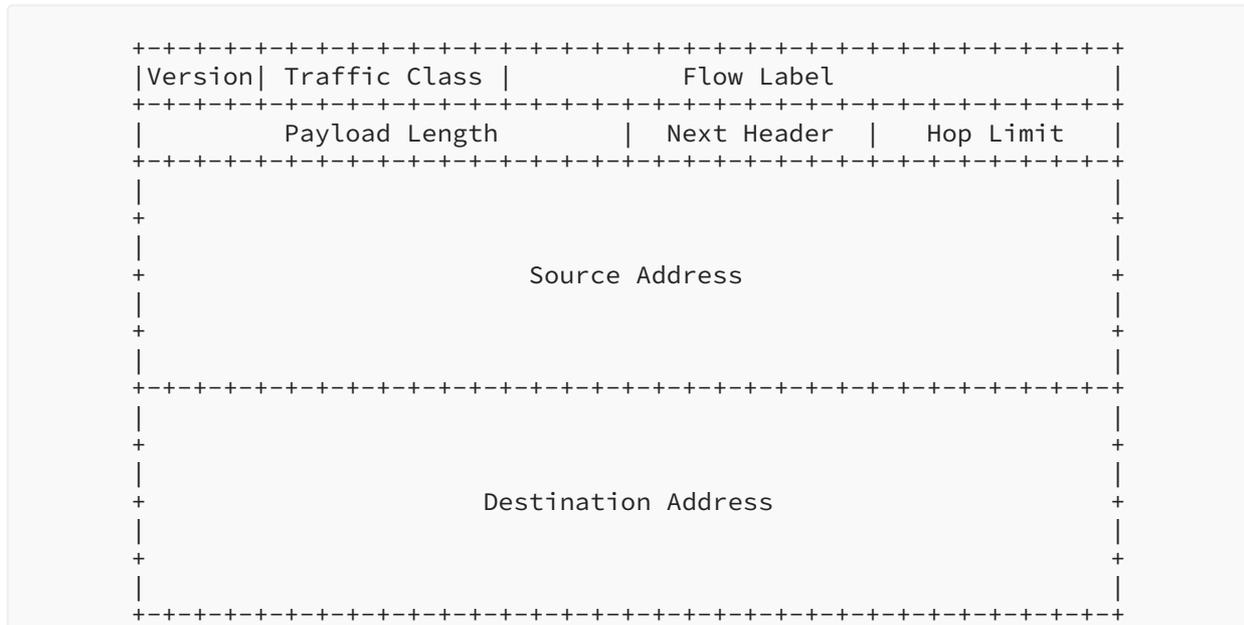
Figure 7: IPv6 Base Header

```
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Code      |          Checksum             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Cur Hop Limit |M|O|  Reserved |        Router Lifetime        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Reachable Time                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                          Retrans Timer                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   Options ...
    +-+-+-+-+-+-+-+-+-+-+-+-
```
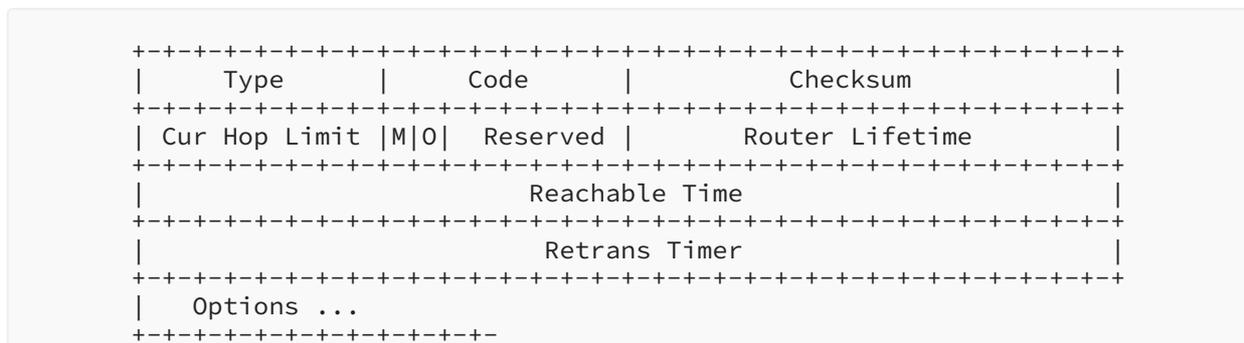
Figure 8: Router Advertisement

The value of the Data Rate field in the Radiotap header is set to 6 Mb/s. This indicates the rate at which this RA was received.

The value of the Transmitter Address in the IEEE 802.11 Data header is set to a 48-bit value. The value of the destination address is 33:33:00:00:00:1 (all-nodes multicast address). The value of the BSS ID field is ff:ff:ff:ff:ff:ff, which is recognized by the network protocol analyzer as being "broadcast". The Fragment number and Sequence number fields together are set to 0x90C6.

The value of the Organization Code field in the Logical Link Control header is set to 0x0, recognized as "Encapsulated Ethernet". The value of the Type field is 0x86DD (hexadecimal 86DD; otherwise, #86DD), recognized as "IPv6".

A Router Advertisement is periodically sent by the router to multicast group address ff02::1. It is ICMP packet type 134. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags, as described in [RFC4861].

The IPv6 header contains the link-local address of the router (source) configured via the EUI-64 algorithm, and the destination address is set to ff02::1.

The Ethernet Type field in the Logical Link Control header is set to 0x86dd, which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01, which is the corresponding multicast MAC address. The BSS ID is a broadcast address of ff:ff:ff:ff:ff:ff. Due to the short link duration between vehicles and the roadside infrastructure, there is no need in IEEE 802.11-OCB to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11-OCB enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.

G.2. Capture in Normal Mode

The same IPv6 Router Advertisement packet described above (monitor mode) is captured on the host in normal mode and is depicted below.

```
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                        Destination...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    ...Destination                |              Source...
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    ...Source                                                 |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Type                |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
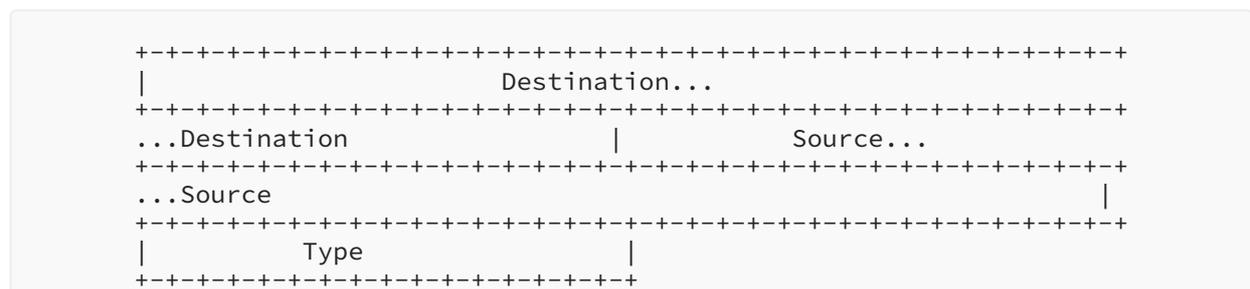
Figure 9: Ethernet II Header

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Version| Traffic Class |              Flow Label               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Payload Length        |  Next Header  |   Hop Limit   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                         Source Address                        +
   |                                                               |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   +                                                               +
   |                                                               |
   +                      Destination Address                      +
   |                                                               |
   +                                                               +
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
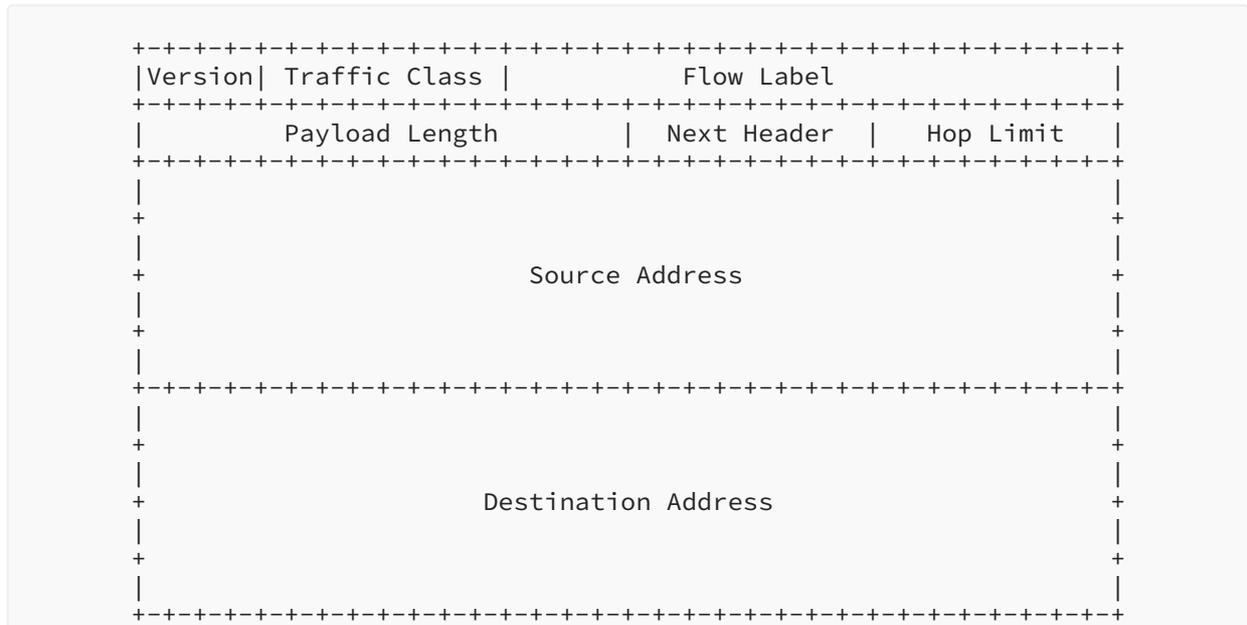
Figure 10: IPv6 Base Header

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |     Code      |           Checksum            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Cur Hop Limit |M|O|  Reserved |        Router Lifetime        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        Reachable Time                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Retrans Timer                         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Options ...
   +-+-+-+-+-+-+-+-+-+-
```
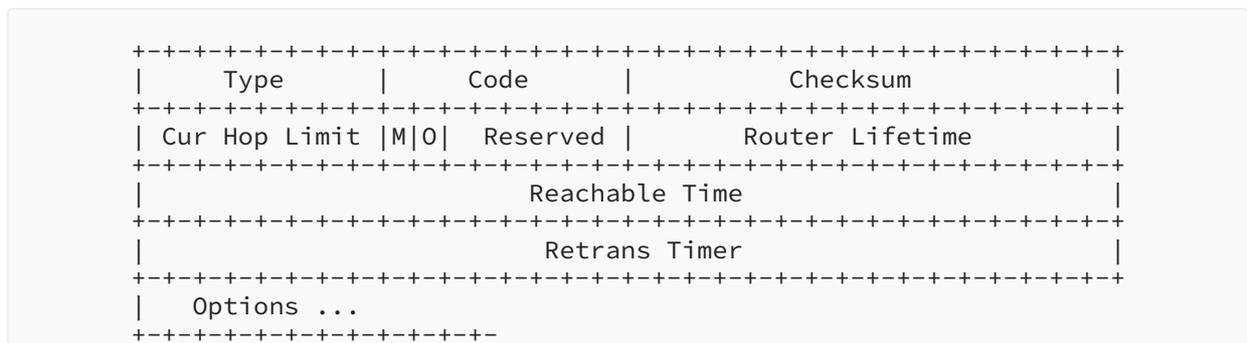
Figure 11: Router Advertisement

One notices that the Radiotap header, the IEEE 802.11 Data header, and the Logical Link Control headers are not present. On the other hand, a new header named the Ethernet II header is present.

The Destination and Source addresses in the Ethernet II header contain the same values as the Receiver Address and Transmitter Address fields present in the IEEE 802.11 Data header in the monitor mode capture.

The value of the Type field in the Ethernet II header is 0x86DD (recognized as "IPv6"); this value is the same as the value of the Type field in the Logical Link Control header in the monitor mode capture.

The knowledgeable experimenter will no doubt notice the similarity of this Ethernet II header with a capture in normal mode on a pure Ethernet cable interface.

A frame translation is inserted on top of a pure IEEE 802.11 MAC layer in order to adapt packets before delivering the payload data to the applications. It adapts 802.11 LLC/MAC headers to Ethernet II headers. Specifically, this adaptation consists of the elimination of the Radiotap, 802.11, and LLC headers and the insertion of the Ethernet II header. In this way, IPv6 runs straight over LLC over the 802.11-OCB MAC layer; this is further confirmed by the use of the unique Type 0x86DD.

Appendix H.   Extra Terminology

The following terms are defined outside the IETF. They are used to define the main terms in the terminology section (Section 2).

DSRC (Dedicated Short Range Communication):
> The US Federal Communications Commission (FCC) Dedicated Short Range Communication (DSRC) is defined in the Code of Federal Regulations (CFR) 47, Parts 90 [CFR-90] and 95 [CFR-95]. This Code is referenced in the definitions below. At the time of the writing of this document, the last update of this Code was dated December 6, 2019.

DSRCS (Dedicated Short-Range Communications Services):
> Radio techniques are used to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the units involved. [CFR-90.7]

OBU (On-Board Unit):
> An On-Board Unit is a DSRCS transceiver that is normally mounted in or on a vehicle or may be a portable unit in some instances. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of [CFR-95] and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of [CFR-95]. OBU operations in the Unlicensed National Information Infrastructure (U-NII) Bands follow the rules in those bands. [CFR-90.7]

RSU (Roadside Unit):
> A Roadside Unit is a DSRC transceiver that is mounted along a road or pedestrian passageway. An RSU may also be mounted on a vehicle or may be hand carried, but it may only operate when the vehicle or hand-carried unit is stationary. Perhaps Furthermore, an RSU is restricted to the location where it is licensed to operate. However, portable or handheld RSUs are permitted to operate where they do not interfere with a site-licensed operation. An RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone when required. [CFR-90.7]

Appendix I.   Neighbor Discovery (ND) Potential Issues in Wireless Links

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861] [RFC4862] was designed for point-to-point and transit links, such as Ethernet, with the expectation of cheap and reliable support for multicast from the lower layer. Section 3.2 of [RFC4861] indicates that the operation on shared media and on NBMA networks require additional support, e.g., for AR and DAD, which depend on multicast. An infrastructureless radio network such as OCB shares properties with both shared media and NBMA networks and then adds its own complexity, e.g., from movement and interference that allow only transient and non-transitive reachability between any set of peers.

The uniqueness of an address within a scoped domain is a key pillar of IPv6 and is the basis for unicast IP communication. [RFC4861] details the DAD method to prevent an address from being duplicated. For a link-local address, the scope is the link, whereas for a globally reachable address, the scope is much larger. The underlying assumption for DAD to operate correctly is that the node that owns an IPv6 address can reach any other node within the scope at the time it claims its address, which is done by sending a Neighbor Solicitation (NS) multicast message, and can hear any future claim for that address by another party within the scope for the duration of the address ownership.

In the case of OCB, there is a potentially a need to define a scope that is compatible with DAD. The scope cannot be the set of nodes that a transmitter can reach at a particular time because that set varies all the time and does not meet the DAD requirements for a link-local address that can be used anytime and anywhere. The generic expectation of a reliable multicast is not ensured, and the operation of DAD and AR as specified by [RFC4861] cannot be guaranteed. Moreover, multicast transmissions that rely on broadcast are not only unreliable but are also often detrimental to unicast traffic (see [IEEE802-MCAST]).

Early experience indicates that it should be possible to exchange IPv6 packets over OCB while relying on IPv6 ND alone for DAD and AR (Address Resolution) in good conditions. In the absence of a correct DAD operation, a node that relies only on IPv6 ND for AR and DAD over OCB should ensure that the addresses that it uses are unique by means other than DAD. It must be noted that deriving an IPv6 address from a globally unique MAC address has this property but may yield privacy issues.

[RFC8505] provides a more recent approach to IPv6 ND, in particular DAD. [RFC8505] is designed to fit wireless and otherwise constrained networks whereby multicast and/or continuous access to the medium may not be guaranteed. [RFC8505], Section 5.6 ("Link-Local Addresses and Registration") indicates that the scope of uniqueness for a link-local address is restricted to a pair of nodes that uses it to communicate and provides a method to assert the uniqueness and resolve the link-layer address using a unicast exchange.

[RFC8505] also enables a router (acting as a 6LR) to own a prefix and act as a registrar (acting as a 6LBR) for addresses within the associated subnet. A peer host (acting as a 6LN) registers an address derived from that prefix and can use it for the lifetime of the registration. The prefix is advertised as not on-link, which means that the 6LN uses the 6LR to relay its packets within the

subnet, and participation to the subnet is constrained to the time of reachability to the 6LR. Note that an RSU that provides internet connectivity **MAY** announce a default router preference [RFC4191], whereas a car that does not provide that connectivity **MUST NOT** do so. This operation presents similarities to that of an access point, but at Layer 3. This is why [RFC8505] is well suited for wireless in general.

Support of [RFC8505] may be implemented on OCB. OCB nodes that support [RFC8505] **SHOULD** support the 6LN operation in order to act as a host and may support the 6LR and 6LBR operations in order to act as a router and in particular to own a prefix that can be used by hosts that are compliant with [RFC8505] for address autoconfiguration and registration.

Acknowledgements

Contributors

Christian Huitema and Tony Li contributed to this document.

Romain Kuntz contributed extensively regarding IPv6 handovers between links running outside the context of a BSS (802.11-OCB links).

Tim Leinmueller contributed the idea of the use of IPv6 over 802.11-OCB for the distribution of certificates.

Marios Makassikis, Jose Santa Lozano, Albin Severinson, and Alexey Voronov provided significant feedback on the experience of using IP messages over 802.11-OCB in initial trials.

Michelle Wetterwald contributed extensively to the MTU discussion, offered the ETSI ITS perspective, and reviewed other parts of the document.

Authors' Addresses

Nabil Benamar
Moulay Ismail University of Meknes
Morocco
Phone: +212670832236
Email: n.benamar@est.umi.ac.ma

Jérôme Härri
EURECOM
06904 Sophia-Antipolis
France
Phone: +33493008134
Email: Jerome.Haerri@eurecom.fr

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan
31066
Republic of Korea
Email: jonghyouk@smu.ac.kr

Thierry ERNST
YoGoKo
1137A Avenue des Champs-Blancs
35510 CESON-SEVIGNE
France
Email: thierry.ernst@yogoko.fr